AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1. (Currently amended) A method for providing identification
2   authentication, comprising:
3   receiving an identification credential from an individual, including a
4   biometric data, wherein the biometric data is stored on the identification
5   credential, and wherein the identification credential is digitally signed with a
6   private key;
7   receiving a biometric sample from the individual;
8   validating the digital signature using a corresponding public key;
9   determining if a difference between the digitally signed biometric data and
10   the biometric data-sample from the individual is below a predetermined threshold;
11   and
12   providing the results of the determination to an interested party;
13   whereby the identity of the individual can be-is authenticated with
14   reference to the identification credential alone, without having to lookup-transmit
15   information for the individual in a databaseover a network.

1   2. (Original) The method of claim 1, further comprising adjusting the
2   predetermined threshold in accordance with instructions received from a user.

1   3. (Currently amended) The method of claim 1, wherein the identification
2   credential can include-includes at least one of a name, a unique ID, a citizenship,

2

3   an issue date, an expiration date, an identifier for an issuing authority, the

4   biometric data, and a digital photo.

1   4. (Currently amended) The method of claim 1, wherein the biometric

2   sample ~~can include~~ includes one of, or a combination of, a fingerprint, a signature,

3   an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

1   5. (Original) The method of claim 1, wherein the digitally signed biometric

2   data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a

3   non-volatile memory, such as flash memory, located on or within the

4   identification credential.

1   6. (Original) The method of claim 1, wherein the digital signature is

2   provided by a central certification authority.

1   7. (Original) The method of claim 1, further comprising granting access to

2   resources based on the determination if the difference between the digitally signed

3   biometric data and the biometric data from the individual is below the

4   predetermined threshold.

1   8. (Currently amended) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to perform a

3   method for providing identification authentication, the method comprising:

4   receiving an identification credential from an individual, including a

5   biometric data, wherein the biometric data is stored on the identification

6   credential, and wherein the identification credential is digitally signed with a

7   private key;

8   receiving a biometric sample from the individual;

3

9   validating the digital signature using a corresponding public key;

10   determining if a difference between the digitally signed biometric data and

11   the biometric ~~data~~ sample from the individual is below a predetermined threshold;

12   and

13   providing the results of the determination to an interested party;

14   whereby the identity of the individual ~~can be~~ is authenticated with

15   reference to the identification credential alone, without having to ~~lookup~~ transmit

16   information for the individual ~~in a database~~ over a network.

1   9. (Original) The computer-readable storage medium of claim 8, wherein

2   the method further comprises adjusting the predetermined threshold in accordance

3   with instructions received from a user.

1   10. (Currently amended) The computer-readable storage medium of claim

2   8, wherein the identification credential ~~can include~~ includes at least one of a

3   name, a unique ID, a citizenship, an issue date, an expiration date, an identifier for

4   an issuing authority, the biometric data, and a digital photo.

1   11. (Currently amended) The computer-readable storage medium of claim

2   8, wherein the biometric sample ~~can include~~ includes one of, or a combination of,

3   a fingerprint, a signature, an iris scan, a facial scan, a voice pattern, a height, a

4   weight, or a palm scan.

1   12. (Original) The computer-readable storage medium of claim 8, wherein

2   the digitally signed biometric data is contained in a magnetic stripe, a bar code, a

3   smart card, a chip-card, or a non-volatile memory, such as flash memory, located

4   on or within the identification credential.

1   13. (Original) The computer-readable storage medium of claim 8, wherein
2   the digital signature is provided by a central certification authority.

1   14. (Original) The computer-readable storage medium of claim 8, wherein
2   the method further comprises granting access to resources based on the
3   determination if the difference between the digitally signed biometric data and the
4   biometric data from the individual is below the predetermined threshold.

1   15. (Currently amended) An apparatus for providing identification
2   authentication, comprising:
3   a receiving mechanism that is configured to receive an identification
4   credential from an individual, including a biometric data, <u>wherein the biometric</u>
5   <u>data is stored on the identification credential, and</u> wherein the identification
6   credential is digitally signed with a private key;
7   a sampling mechanism that is configured to receive a biometric sample
8   from the individual;
9   a validation mechanism that is configured to validate the digital signature
10   using a corresponding public key;
11   a determination mechanism that is configured to determine if a difference
12   between the digitally signed biometric data and the biometric ~~data~~ <u>sample</u> from
13   the individual is below a predetermined threshold; and
14   a feedback mechanism that is configured to provide the results of the
15   determination to an interested party;
16   whereby the identity of the individual ~~can be~~ <u>is</u> authenticated with
17   reference to the identification credential alone, without having to ~~lookup~~ <u>transmit</u>
18   information for the individual ~~in a database~~<u>over a network</u>.

1   16. (Original) The apparatus of claim 15, further comprising an adjustment

2 mechanism configured to adjust the predetermined threshold in accordance with

3 instructions received from a user.

1   17. (Currently amended) The apparatus of claim 15, wherein the

2 identification credential ~~can include~~ includes at least one of a name, a unique ID, a

3 citizenship, an issue date, an expiration date, an identifier for an issuing authority,

4 the biometric data, and a digital photo.

1   18. (Currently amended) The apparatus of claim 15, wherein the biometric

2 sample ~~can include~~ includes one of, or a combination of, a fingerprint, a signature,

3 an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

1   19. (Original) The apparatus of claim 15, wherein the digitally signed

2 biometric data is contained in a magnetic stripe, a bar code, a smart card, a chip-

3 card, or a non-volatile memory, such as flash memory, located on or within the

4 identification credential.

1   20. (Original) The apparatus of claim 15, wherein the digital signature is

2 provided by a central certification authority.

1   21. (Original) The apparatus of claim 15, further comprising a security

2 mechanism configured to grant access to resources based on the determination if

3 the difference between the digitally signed biometric data and the biometric data

4 from the individual is below the predetermined threshold.

6